(12/31/1995)

DECLASSIFIED BY 60324/UC/baw/sab/as
ON 09-21-2012

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/04/1998

To: NSD/CID **Attn:** SSA [redacted]
OSIIP/CITAC/Rm 11887

From: Sacramento
WCC, Squad 5
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :mah

Case ID # (U) ~~(S)~~ 288-HQ-1242560-167 (Pending)
(U) ~~(S)~~ 288-SC-30782-SUB X (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO;HQ

Synopsis: (U) ~~(S)~~ Information possibly pertaining to intrusions into DOD Domain Name Servers using the "statd" exploit on Solarus 2.4 operating systems.

(U) ~~(S)~~ ~~**Classified By: 10877, 4/sc**~~
~~**Reason : 1.5(c)**~~
~~**Declassify On: 03/04/2008**~~

Reference: (U) ~~(S)~~ HQ EC's dated 2/9/98, and 2/12/98.

Enclosures: (U) ~~(S)~~ Enclosed for FBIHQ/CITAC are the following:

1) 22 pages of logs provided by University of California-Davis.

2) 3 logs provided by the University of Colorado-Boulder. (encloses sent to CA)

Details (U) ~~(S)~~ On 2/2/98, [redacted] Computer Security Analyst, Information Resources, Division of Information Technology, University of California, 1 Shields Avenue, Davis, California, 95616, telephone [redacted] advised all 17,000 computers in the University of California-Davis (UCD) network have been attacked using a "statd" probe between 1/25/98 and 1/28/98. Page 6 of enclosure 1, UCD Incident Response Team (UCDIRT) notice #63, identified the initial probes as originating from netgate.saes.com. The initial attack lasted almost twenty-four hours. Three UCD hosts (ging.ucd.edu, b6 b7C

~~SECRET~~

UPLOADED

junior.itd.ucdavis.edu, and guardian.ucdavis.edu) had TCP connections to other services during the attack. The Sun remote procedure connections from saes.com were the only ones logged in for that week. Saes.com was registered to St. Andrews School, Bethesda, Maryland. [redacted] was identified as the technical contact.

(U) (S) In the opinion of [redacted] UCDIRT leader, this attack was probably used to generate a list of hosts running "statd." The "statd" systems were then hit from computers located at Harvard University and Columbia University. Pages 7 through 10 of enclosure 1, identify the two computers at Harvard and Columbia as scotia.harvard.edu, and bone.tc.columbia.edu. Three hosts were intruded. The compromised computers were running Solaris 2.4.

(U) (S) [redacted] was the administrator for one of the compromised hosts in the Geology Department. After replacing Solaris 2.4 with Solaris 2.5.1, [redacted] examined logs from January 17, and 18, 1998. [redacted] discovered another "statd" attack. On January 18, 1998, the intruder gained root access. The origin of the attack appeared to be [redacted] Pages 4 and 5 of enclosure 1 represent examples of the "statd" attacks which occurred on January 17, and 18. b6 b7C

(U) (S) [redacted] Associate Professor, Department of Computer Science, reviewed logs and discovered "imapd" probes during January 18, 1998, from [redacted] Page 3 of enclosure 1 is [redacted] addendum to UCDIRT notice #63. According to [redacted] "imapd" programs serve the same purpose as "statd" programs, that is, port mapping.

(U) (S) Likewise, another UCD administrator, [redacted] reviewed logs and discovered additional attempted "imapd" probes as early as November 18, 1997. The origin of these "imapd" probes appeared to be [redacted] Pages 1 and 2 of enclosure 1 is [redacted] addendum to UCDIRT notice #63.

(U) (S) Sacramento provided relevant UCD logs to the following:

1) [redacted] Columbia University, [redacted] administrator for bone.tc.columbia.edu.

2) [redacted] Harvard University, [redacted]

[redacted] administrator for scotia.harvard.edu.

3) [redacted] St. Andrews, [redacted] administrator for netgate.saes.com.

(U) ~~(S)~~ [redacted] provided pages 18, 19 and 20 of enclosure 1. [redacted] noted, SA [redacted] FBI Cleveland, [redacted] had also requested this information. SA [redacted] was contacted. SA [redacted] confirmed he was aware of Columbia's information, and had traced the intruder to [redacted] in [redacted] SA [redacted] was preparing to serve a search warrant on the subscriber. SA [redacted] was also advised the [redacted] intruder had successfully penetrated the UCD computer used for campus events and visitor services, had created a directory called /home/meta and a password entry name of [redacted] According to SA [redacted] this was the leitmotiv of his intruder. Pages 15, 16, and 17 of enclosure 1 were provided to SA [redacted]

(U) ~~(S)~~ [redacted] Harvard University, advised he had no logs for scotia.harvard.edu. [redacted] St. Andrews, likewise advised he had no logs for netgate.saes.com. However, [redacted] added he had been contacted by [redacted] University of Colorado-Boulder.

b6
b7C

(U) ~~(S)~~ [redacted] University of Colorado-Boulder, [redacted] provided enclosure 2. [redacted] advised his network had been the target of a "statd" probe from netgate.saes.com, computer [redacted] The three compromised University of Colorado machines were all running Solaris 2.4+.

(U) ~~(S)~~ On 2/26/98, UCD Computer Security Analyst [redacted] was asked if the University had any indication their UCD machines had been used to launch flood attacks on any other computer networks. [redacted] said they had received a few complaints concerning some internet relay channels which had been flooded, but nothing else. On the other hand, [redacted] pointed out the UCD computers logged only TCP/telnet connections. Therefore, [redacted] did not believe UCD Administrators would be aware of any ping attacks launched from their networks. [redacted] added, UCD Administrators could track something other than standard TCP/Telnet connections only if the suspect activity occurred coincident with the tracking.

(U) ~~(S)~~ Sacramento is attempting to identify the subscriber who launched the "statd" probes from

To: NSD/CID From: Sacramento
Re: (U) ~~(S)~~ 288-HQ-1242560, 03/04/1998

[redacted] Any other leads will be left to the discretion of OSIIP/CITAC. b6 b7C

◆◆